

REMARKS

This is in response to the Final Office Action mailed on September 28, 2007. Claims 1 and 3-23 were pending in that action and all claims were rejected. Claims 1, 3-13 and 21-23 were rejected under 35 USC §103(a) as being unpatentable over Sutter (US 6,446,092, hereinafter Sutter) and further in view of Nguyen et al. (US, 7,194,621, hereinafter Nguyen). Claims 14-20 were rejected under 35 USC §102 as being anticipated by Sutter. In this response no claims have been amended. With the present response, all claims remain unchanged.

The present application pertains to systems and methods for storing sensitive data in a database. In one aspect of the invention individual authorized application users are each aligned with their own version of an application-wide security key such that it becomes unnecessary to directly store the key in its original form. In one embodiment, the underlying security key is used to process sensitive data (emphasis added). In one embodiment, the user's version of the application-wide security reflects an encryption-based relationship to the user's password.

Independent claim 1 recites a method that includes receiving a password from a user. The password is utilized as a basis for generation of a user-specific version of an encryption component (emphasis added). As claimed, the encryption component is a collection of data that specifies an encryption or decryption process. Further, as claimed, a user is selectively allowed to process the user-specific version of the encryption component so as to derive the encryption component (emphasis added). This allows the user to utilize the original encryption component, separate from the password (emphasis added). Finally, as claimed, the original encryption component is utilized to process sensitive data. This allows the user to utilize the original encryption component that was generated for the specific user.

The Sutter reference pertains to a distributed database system. The bulk of the referenced is focused on describing details of data management within the distributed system. Very little of the description has anything to do with database security. There is, as pointed out in the Office Action, some description of database security in certain sections of the Sutter reference. Sutter does describe receiving a password from a user.

The Examiner argues that the reference shows the password being utilized to generate some sort of a user-specific version of an encryption component. Even if this is true, other elements of independent claim 1 are still missing from the reference. In the office action, the Examiner points to Sutter at cols. 87 and 15 as teaching “selectively allowing the user to process the user-specific version of the encryption component and so as to derive the encryption component. Similarly, the Examiner indicates Col. 73 and Col. 74 as showing “utilizing the encryption component to process sensitive data.” The Examiner notes that Col. 87, lines 39-45 teach that a developer can selectively encrypt the database contents at varying levels of granularity. However, it is respectfully pointed out that these passages, and indeed the entire Sutter reference, fail to teach or suggest any subsequent utilization of the original encryption component that was combined with the developer password.

Col. 51 lines, 21-67 of the Sutter reference does indicate that a password hash can be used along with a private key which is encrypted, but there is no teaching or suggestion that additional sensitive information is processed using the same encryption or password hash. Col. 15, lines 50-55 of Sutter does indicate that a database can include a set of activities to allow users to easily find and choose data they need, but this has little if anything to do with the claimed database security features. Col. 73 lines 50-56 of Sutter does recite using a PermissionID to determine whether the site or user has a requisite permission, but it does not teach of using the original encryption component to process sensitive information. Col. 74 lines 60-67 also discuss a way to use Site permissions to enable an application designer and administrators to deal with sensitive information to ensure that they are only modified at one site. This does not disclose utilizing the original encryption component to process sensitive information.

For further clarification, Applicant has included in an Appendix A to the present response a series of diagrams illustrating significant differences between the elements of Applicant's claim 1 and teachings of the cited Sutter reference. For at least the reasons noted herein, it is respectfully submitted that independent claim 1 is in a condition for allowance.

Claim 14 recites a method that includes creating and storing a plurality of user-specific versions of an encryption component. As claimed, users are selectively allowed to process

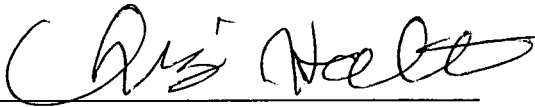
their version of the encryption component so as to derive the encryption component. The encryption component is then utilized to process sensitive data. For reasons similar to those discussed above in relation to claim 1, it is respectfully submitted that independent claim 14 is in condition for allowance as well.

Independent claim 21 pertains to a computer implemented method of providing data security which includes receiving a password from a user, processing the password to form an encrypted version and utilizing the password as basis for decrypting a user-specific version of an encryption component if the encrypted version matches an authorized value stored in a database. The Office Action indicated that the encrypted version of the password is compared to a list of authorized values stored in a database is recited in Sutter at Col. 51 lines 21-67 and Col. 74, lines 60-67. Sutter recites in particular at Col. 51 lines 57-64 that “[b]ecause the private key structure contains redundant information that will let us know that we have decrypted it correctly, there is no need to store even a hash of the user signing password.” This indicates that the encrypted version of the password is in fact decrypted before it is compared to a list of authorized values since no hashed version of the signing password is stored. This portion of Sutter in fact teaches away from comparing an encrypted version of the password to authorized values, since it indicates that it is not necessary to store an encrypted version of the password. Col. 74 , lines 60-67 indicate that site permissions are provided to application designers and administrators, but this does not indicate that the encrypted password is verified against authorized values. It is respectfully submitted that independent claim 21 is in form for allowance for at least these reasons.

In summary, for at least the reasons outline herein, it is respectfully submitted that claims 1 and 3-23 are in condition for allowance. The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: 

Christopher L. Holt, Reg. No. 45,844
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312